Release Notes

NetEnforcer™ System Version 3.0

This document details some issues, problems and clarifications to the current product release, its features and associated product-specific documentation. Please review documents on the WEB at http://www.allot.com/documents for an up-to-date list of known issues with your specific release.

New Products and Features in Release 3.0

The following features have been added to release 3.0 from the previous 2.1.1 release. Please consult the user manual for details on each of these features.

New Features for the NetEnforcer System

- **New Look Case**
  The NetEnforcer now comes in a new case along with a new name. All connectors are now placed on the front panel, instead of the rear.
- **Hardware Bypass**
  The Hardware Bypass is an add-on PCI card for AC200 and AC300 Systems that fits in the spare slot on the AC System's main board. For AC101, AC201 and AC301 systems, the Hardware Bypass is built in. The AC Software will analyze the AC System and determine its operational state. If the AC Software determines that the AC System is unresponsive, it will activate the Hardware Bypass which will re-route traffic to bypass the AC System. The Hardware Bypass will also activate if there are any hardware problems, such as power failure. The Software bypass option is still available.
- **Bi-directional Support**
  This allows separate shaping, monitoring and accounting based on traffic direction.
- **Full Mesh Mode**
  The NetEnforcer will now operate in complex network environment such as a Full Mesh Environment. Such environments force the NetEnforcer to limit its functionality and it will not support Load Balancing, Cache Redirection and Content Inspection rules. This is due to the fact that not all the traffic passes through the AC in these environments.
- **Unidirectional TCP traffic**
  The NetEnforcer now supports hybrid satellite and CTV hybrid networks where not all the traffic passes through the NetEnforcer.
- **Any IP- and non-IP support**
  The NetEnforcer now supports non-UDP and non-TCP traffic, as well as allowing shaping of protocols that run over Ethernet, such as IPX, SNA, etc.
- **Broadcast/Multicast Shaping**
  The NetEnforcer now supports the shaping of Broadcast/Multicast IP traffic.

- **Dynamic DNS Support**
  The NetEnforcer now supports DNS incorporated with DHCP.
- **LDAP and COPS**
  The NetEnforcer now includes an LDAP/COPS client, along with the ability to create Virtual Channels automatically from LDAP and IP address based definitions.
- **Policy and Operation Line Interface**
  You will now be able to define Virtual Channels and Catalog rule entries via the Command Line Interface.
- **Remote VC definition**
  The NetEnforcer has the ability to save its configuration on a remote server using TFTP. It can then load this configuration later from the remote server.
- **Access Control Catalog**
  The Access Control Catalog has been removed. The Access options Pass-As-Is, Reject and Drop are available from within the QoS and Connection Control Catalogs.
- **DHCP Support**
  You can now set the configuration of the NetEnforcer via Dynamic Host Configuration Protocol. This enables the NetEnforcer to receive an IP address, subnet mask, router address and Domain Name Server (DNS) addresses from the DHCP server.
- **Port Range Support**
  You can now define services using a range of TCP/UDP ports. This can be used to support applications with port negotiation that are not explicitly supported by the system, such as X-Windows and multimedia applications.
- **ToS Support**
  The NetEnforcer now supports ToS marking and ToS based classification per connection.

Improved Features for the NetEnforcer

- **Configuration Improvements**
  Network Interfaces and Bridging are now the only areas in the configuration of the NetEnforcer that require you to reset the NetEnforcer. They are also marked either as *Current* or *Saved*, indicating whether the configuration is the current one or the one that will exist after reboot.
- **Administrator Setup**
  The Administrator Setup has been considerably improved, to make it easier for Network Administrators with or without browser access to set up and maintain the NetEnforcer.
- **Performance Improvements**
  The AC301 System now supports 64000 simultaneous connections, 1000 connection creations per second, and traffic rates up to 60 Mbps for short packets and 100 Mbps for long packets.
- **Bridge Mode Improvements**
  The NetEnforcer now features improved configuration, including one IP address for both Ethernet interfaces.
- **IP options Support**
  The NetEnforcer will now pass IP options transparently, supporting the ***traceroute*** utility.

- **Improved Security**
  The NetEnforcer now features password encryption, and limiting access to the User Interface from a list of authorized IP addresses. The IP address of the host of the current browser connection to the NetEnforcer will be automatically added to the allowed hosts list, to prevent self-lockout.
- **Maximum Bandwidth per connection support**
  You can now specify the maximum bandwidth to be assigned per connection, along with defining burst and CBR traffic types.

URGENT:
When upgrading from a previous version of the software, the installation procedure will overwrite your Virtual Channel database with the default database. Your original database is saved to: /tmp/my_database.dd.mm.yy.tgz. If you wish to restore your database after the installation procedure is complete, email this file us at support@allot.com, subject: Convert Database to 3.0.

At the start of the installation, the installation procedure will inform you of the fact that your database will be overwritten, and will ask you if you wish to proceed with the upgrade. If you answer yes, your old database will be saved to the file, and then replaced by the default database. If you answer no, your database will be saved to a file, and the installation procedure will exit.

PLEASE READ:

Notes on JAVA Plugin

- You must download and install the Java plug-in from the main menu prior to running the Virtual Channel editor, Monitoring or Accounting Java applications.
- It is recommended that you use PCs with at least 64M of RAM.
- You should set the memory of the Java plug-in to the maximum RAM on your PC before running the Web interface. After downloading and installing the Java plug-in:
  - From your windows PC, select
    Start->Programs->Java Plug-in control panel
  - In the ***basic*** palette, in the field labeled :
    JAVA Run-Time Parameters
    Enter in the box the amount of RAM on your PC in the format:
    -mx <PC RAM size>
    where <PC RAM size> is the size of RAM on your PC.
  - Select OK
  - Restart the browser

Known Issues in Version 3.0

Following is a list of known problems in software version 3.0.

- Do NOT use the access control option Reject. Use Drop instead. Using reject will cause the NetEnforcer to crash.
- If the Monitoring module loses its connection to the NetEnforcer, an error message will appear after ten minutes informing you that the connection has been lost. You will need to restart your browser to reestablish the connection.
- Your DHCP server must be located on the same interface of the NetEnforcer as your default router. If the server is located on the second interface, the NetEnforcer will not be able to contact it. If this is your network configuration, you will have to set network settings manually.
- IP's that have no name resolving are not written to the Accounting database, and so cannot be viewed via ODBC.
- Currently, there is no warning informing you of the length of time needed to generate a report in the Bandwidth Accountant. A large report may take over 15 minutes to be generated.
- In the Bandwidth Accountant, FTP entries are divided into control and data connections.
- The Load Balancing and Cache Redirection features are currently unavailable.
- Heavy loads and a large number of connections affect the accuracy of the Priority per Connection feature. For most accurate results, we recommend setting priority per VC.
- Defining a VC according to HTTP header content, such as a specific URL, may fail if the responses are very small. In such a case, the HTTP service will match the traffic, or if there is no VC with HTTP defined, the traffic will fall under the Fallback rule.
- When several different services with the HTTP protocol but with separate URLs or methods are defined, the protocol distribution chart will show all HTTP traffic as associated with one of the defined services only.
- Currently the reports generated by the Bandwidth Accountant may be subject to inaccuracies with regard to the exact amount of traffic transferred through a VC within a given time period. Also, when using Dynamic DNS, some inaccuracies in the resolution of host names to IP addresses may occur.
- Host definitions using the wildcard character '*' should now be defined as a range or a subnet instead.

Important Clarifications

1. We strongly recommend that you do not alter the default Time Resolution Recording Frequency in the Database Recording Parameters of the Bandwidth Accountant. Increasing the default value (1 hour) can lead to serious problems in the Accounting and Monitoring applications. Further, we recommend you use the RADIUS protocol to export accounting data to a RADIUS server. This will keep resources available by writing the data to the client machine instead of the NetEnforcer.
2. The Fallback rule cannot be changed. If you wish for traffic falling under this VC to be given an access policy or QoS other than that given by the Fallback VC, add another VC above it with the same rule matching, and define your preferred access policies and QoS.

3. When connecting the AC to a hub or switch port, you must use a “straight-through”, direct cable. When connecting the NetEnforcer directly to a router, firewall, server or other host equipment, you must use a “cross-over” type cable.
4. The accounting database may, at times, get very large and take excessive time to download via ODBC. By defining filters and compressing the data frequently, you can improve the performance of accounting.
5. Any computers located on the external interface that communicate directly to the NetEnforcer (e.g., telnet client or a browser) must be defined as specific hosts using the hosts list feature in AC Config or administrator setup.
6. When working with traffic that consists of very short connections (one or two packets per connection) it is recommended to use the “Minimum per VC” quality rather than the Priority scheme.
7. When defining a VC to be active only during specific time periods, it is important to be aware that the VC is applied only to new connection attempts. Any existing connections that may otherwise fall under that VC will continue to pass under their original VC. In the case of a reject (or drop) policy being applied, no existing connections that have already been matched to an alternative VC, but now correspond to the new VC, will be disconnected.
8. If you wish to define, in the Service Catalogue Editor, two identical services with different names, the following must be observed: both entries must have the same Application Protocol, and the same Advanced Parameters (timeouts).
9. If a Virtual Channel is deleted then all traffic passing through that Virtual Channel will be removed from the Monitoring screen. Traffic that has previously been displayed on the Monitoring screen under that VC will also be removed from the Monitoring screen. Any existing connections falling under that VC will also be removed from the Monitor.
10. Monitoring will also display Non-TCP (and Non-IP) traffic. Unlike TCP this traffic does not acknowledge connection closure. Therefore the closure of such connections is indicated by a pre-determined period of inactivity. Therefore, until this timeout period has expired the connections will participate in the connection count on the monitoring screen.

Frequently Asked Questions

The following are some common issues and questions of the NetEnforcer. If you have any questions you would like answered, please email all questions to support@allot.com.

Serial Port Connection Questions

Q: Why can I not connect through my serial port to the NetEnforcer?

A: Make sure you use the female-female connector that came with your unit and that your terminal or terminal emulation software (such as HyperTerminal on a PC setup in VT100 emulation mode) is set to 19200 baud, 0 stop bits, no flow control and no parity. Note that the “erase” key is the <delete> button on your keyboard.

Screen Display Questions

Q: When I connect to the NetEnforcer through my WEB browser, the screen does not display properly.

A: First, please make sure you have downloaded the correct version of the WEB browser. In general, the product has been fully tested with both Netscape and Internet Explorer versions 4 and above. You must also install the correct "Java Plug-in". The first time you login via your specific WEB browser to the NetEnforcer and view the front panel display, you must select the button that is labeled "Install Java Plug-In First". Make sure you have set your JAVA Plug In memory to the maximum RAM on your system (see note above).

In addition, the Java-based applications including the VC Definition Editor, Monitoring and Accounting work best when your system is set to at least 256-color palettes and 800X600-pixel resolution.

Q: On some of my screens, there is a message "Warning: Applet Window". Is this OK?

A: This is a normal Java message that informs you that the Java Applet is unsigned. If you want to remove it, you must install the Security Key. **Select Install Java plug-in and security key first…** from the NetEnforcer Main screen and follow the on-screen directions.

Q: I have many VC rules defined and my User Interface is very slow.

A: You can speed up the performance of the VC screen by making the size of the displayed screen to a smaller size.

Monitoring Questions

Q: Monitoring shows a Virtual Channel using more bandwidth than has been assigned to it. Why?

A: This can be due to two reasons. The first is a situation where the length of the incoming Ethernet packet is greater than the maximum bandwidth assigned to the Virtual Channel. As at least one packet has already been passed (needed for rule matching and Virtual Channel assignment), the NetEnforcer increases the maximum bandwidth of the Virtual Channel to that of the packet size. For example, if the size of the packets for a Virtual Channel is 1518 bytes (the maximum size for an Ethernet packet), and the maximum bandwidth assigned to the Virtual Channel is 1.2 Kbytes per second, then the bandwidth for that Virtual Channel will be increased to 1518 bytes per second, and this will be shown in the Monitoring screen.

The second situation is where the size of the packet is not an exact fraction of the maximum bandwidth assigned to the Virtual Channel. In this case, instead of sending a fraction of the final packet, the bandwidth will be increased to allow the whole of the final packet to pass through the Virtual Channel. For example, if you have assigned a maximum bandwidth of 40Kbits per second to a Virtual Channel, and the packet length is 12Kbits (1.5Kbytes), then instead of passing three whole packets and a fraction of the fourth, the NetEnforcer will increase the bandwidth of the Virtual Channel to 48Kbits per second, to allow four packets to pass.

Bandwidth Management Questions

Q: What happens when I allocate a minimum bandwidth on a connection or Virtual Channel?

A: The NetEnforcer will allocate only the bandwidth that is required for a given connection. If, for example, a connection is guaranteed a minimum of 50Kbytes/sec, but is currently only using 25Kbytes/sec, the rest of the bandwidth will be used by other connections. This means that other connections can "borrow" bandwidth from other underutilized connections with guaranteed rates. When the "guaranteed" connections need more bandwidth, they will get that guaranteed minimum rate.

Q: What happens if I allocate more Virtual Channel minimum bandwidth guarantees than my line speed can support?

A: Each time a new connection is initiated that is part of a non-active Virtual Channel with minimum bandwidth guarantees, that Virtual Channel will now be assigned its minimum bandwidth up to the maximum capabilities of the line. If the newly activated Virtual Channel requires bandwidth that is beyond the maximum of the line rate, all subsequent connections that are part of that Virtual Channel will be given the specific action defined (reject, deny or assign it the given priority).

List of Known Problems and Workarounds

1. *Problem: Rule located at position 256 is ignored.*
   Solution: Within the Virtual Channel Table, the rules at position 256 or any multiple thereof (512, 768, etc.) are ignored. Thus, if you have more than 255 rules within your VC Table, enter a rule in position 256 that no traffic matches. Rule matching will then continue from rule 257 onwards. Repeat this for rules located at multiples of 256.
2. *Problem: Setting applications to very low priorities (1-2) may cause applications to disconnect.*

   Solution: The difference between the highest priority applications and the lowest priority applications should usually be very small (1-2 steps). Large differences in priority (9 or 10 steps), for many applications, may cause excessive timeouts.
3. *Problem: AC System equipped with bypass is permanently in bypass mode.*
   Solution: first, ensure that the hardware bypass is configured. Enter the administrator setup, and select option 3 from the Setup menu. Answer yes to the question "Does the NetEnforcer have a card for hardware-bypass?", and answer no to the question "Enable software bypass?".
   Second, ensure that the following files exist on the AC System:
   /usr/local/SWG/etc/flags: **`ac-has-hwbypass`**. This file tells the AC System a hardware bypass has been installed.
   /usr/local/SWG/etc/flags: **`on-bypass-hwbypass`**. This file tells the AC System to use the Hardware Bypass in place of the Software Bypass.
   If the problem persists, try swapping the data cables between ETH0 and ETH1. If none of these solutions work, contact our customer support service at support@allot.com.